

**Abstract of JP 11-252158**

**Problem to be solved:** To simply extract information required for transmission/reception such as an electronic mail address and to check a computer virus or the like in a stage before the electronic mail reaches a recipient.

**Solution:** In this electronic mail information management method, electronic mail information sent/received is analyzed to detect items consisting of the electronic mail information (step s1), an electronic mail address and a name of a sender/recipient are extracted as the information used in common by plural users using in common an electronic mail server and formed to be a database from the items consisting of the electronic mail information (step s2). Furthermore, processing in response to the item such as a virus check is applied to the items consisting of the electronic mail information (a main text and an added sentence part) (steps s3, s4), when the electronic mail information is proper, it is sent to an electronic mail server (steps s5, s6) and when the electronic mail information is improper, the electronic mail information is deleted (steps s5, s7).

(51) Int.Cl. <sup>8</sup>	識別記号	F I	
H 0 4 L 12/54		H 0 4 L 11/20	1 0 1 B
12/58		G 0 6 F 9/06	5 5 0 Z
G 0 6 F 9/06	5 5 0	12/14	3 1 0 Z
12/14	3 1 0	13/00	3 5 1 G
13/00	3 5 1		3 5 1 Z

審査請求 未請求 請求項の数 7 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願平10-48411

(22) 出願日 平成10年(1998) 2月27日

(71) 出願人 000002369

セイコーエプソン株式会社

東京都新宿区西新宿 2 丁目 4 番 1 号

(72) 発明者 水谷 憲司

長野県諏訪市大和 3 丁目 3 番 5 号 セイコーエプソン株式会社内

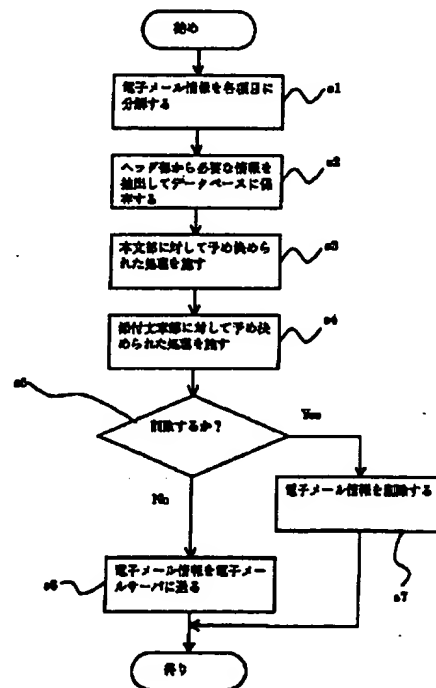
(74) 代理人 弁理士 鈴木 喜三郎 (外 2 名)

(54) 【発明の名称】 電子メール情報管理方法及び装置並びに電子メール情報管理処理プログラムを記録した記録媒体

(57) 【要約】

【課題】 電子メールアドレスなど送受信に必要な情報を簡単に取り出せるようにするとともに、コンピュータウイルスなどのチェックを受信者に届く前の段階で行う。

【解決手段】 送受信される電子メール情報を解析して、電子メール情報を構成する項目を検出し（ステップ s 1）、その電子メール情報を構成する項目から当該電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報として送受信者の電子メールアドレスや名前を取り出してデータベース化する（ステップ s 2）。また、その電子メール情報を構成する項目（本文部や添付文章部）に対し、ウイルスチェックなどその項目に応じた処理を施し（ステップ s 3、s 4）、電子メール情報が適切で有ればそれを電子メールサーバに送り（ステップ s 5、s 6）、不適切であれば電子メール情報を削除する（ステップ s 5、s 7）。



#### 【特許請求の範囲】

【請求項1】 少なくとも2つの電子メールサーバ間で送受信される電子メール情報を管理する電子メール情報管理方法において、

送受信される電子メール情報の送信時または受信時に、その電子メール情報を解析して、電子メール情報を構成する項目を検出し、その電子メール情報を構成する項目から、或る電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を取り出し、当該電子メールサーバを共通に用いるそれぞれのユーザが管理するそれぞれのコンピュータからアクセス可能に保存するとともに、その電子メール情報を構成する項目のうち、予め定められた項目に対し、その項目に応じた処理を施すことを特徴とする電子メール情報管理方法。

【請求項2】 前記或る電子メールサーバを共通に用いるユーザが共通に利用できる情報は、発信者と受信者の少なくとも一方の側の電子メールアドレスとその名前を含むことを特徴とする請求項1記載の電子メール情報管理方法。

【請求項3】 前記電子メール情報を構成する項目のうち、予め定められた項目に対しその項目に応じて施す処理は、

前記予め定められた項目にコンピュータウイルスが存在するか否かのチェックと、その電子メール情報を受信者に配布すべきか否かを判断するために前記予め定めた項目の内容チェックの少なくとも一方を行い、チェック結果が適正であると判断した場合は、その電子メール情報を前記受け取り側の電子メールサーバに送り、コンピュータウイルスが存在する場合は、コンピュータウイルスの影響を除去したのち、前記受け取り側の電子メールサーバに送り、コンピュータウイルスが除去できない場合、または、前記予め定めた項目の内容が受信者に配布すべきでない内容であると判断された場合は、当該電子メールを削除することを特徴とする請求項2または3記載の電子メール情報管理方法。

【請求項4】 少なくとも2つの電子メールサーバ間で送受信される電子メール情報を管理する電子メール情報管理装置において、

送受信される電子メール情報を解析して、その電子メール情報を構成する項目を検出し、その電子メール情報を構成する項目から、或る電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を取り出すとともに、前記電子メール情報を構成する項目のうち、予め定められた項目に対しその項目に応じた処理を施す電子メール情報解析手段と、

この電子メール情報解析手段によって取り出された前記或る電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を、これらユーザがそれぞれ管理するそれぞれのコンピュータからアクセス可能に保存するデータ記憶手段と、

を有することを特徴とする電子メール情報管理装置。

【請求項5】 前記電子メール情報解析手段が取り出す当該電子メールサーバを共通に用いるユーザが共通に利用できる情報は、発信者と受信者の少なくとも一方の側の電子メールアドレスとその名前を含むことを特徴とする請求項4記載の電子メール情報管理装置。

【請求項6】 前記電子メール情報解析手段が行う電子メール情報を構成する項目のうち、予め定められた項目ごとにその項目に応じて施す処理は、

前記予め定められた項目にコンピュータウイルスが存在するか否かのチェックと、その電子メール情報を受信者に配布すべきか否かを判断するために前記予め定めた項目の内容チェックの少なくとも一方を行い、チェック結果が適正であると判断した場合は、その電子メール情報を前記受け取り側の電子メールサーバに送り、コンピュータウイルスが存在する場合は、コンピュータウイルスの影響を除去したのち、前記受け取り側の電子メールサーバに送り、コンピュータウイルスが除去できない場合、または、前記予め定めた項目の内容が受信者に配布すべきでない内容であると判断された場合は、当該電子メールを削除することを特徴とする請求項4または5記載の電子メール情報管理装置。

【請求項7】 少なくとも2つの電子メールサーバ間で送受信される電子メール情報を管理する電子メール情報管理処理プログラムを記録した記録媒体であって、その処理プログラムは、

送受信される電子メール情報の送信時または受信時に、その電子メール情報を解析して、電子メール情報を構成する項目を検出する手順と、

その電子メール情報を構成する項目から、或る電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を取り出す手順と、

これによって取り出された情報を、当該電子メールサーバを共通に用いるそれぞれのユーザが管理するそれぞれのコンピュータからアクセス可能に保存する手順と、

その電子メール情報を構成する項目のうち、予め定められた項目に対しその項目に応じた処理を施す手順と、

を含むことを特徴とする電子メール情報管理処理プログラムを記録した記録媒体。

#### 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク上の電子メール情報を、システム側で自動的に管理する電子メール情報管理方法及び装置並びに電子メール情報管理処理プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】従来の電子メールシステムは、概略的には図4に示すような構成となっている。このようなシステムにおいて、たとえば、B社のユーザb1がA社のユーザa1宛に電子メール情報を送ることを考える。

【0003】この場合、ユーザb1は自己の管理するクライアントコンピュータ（以下、パソコンという）PC1を用い、電子メールソフトS1を起動することにより電子メール情報の発信がなされるが、その発信された電子メール情報は、電子メールサーバB1から、この図4の例では公共ネットワーク1を通してA社の電子メールサーバA1に蓄わえられる。そして、ユーザa1は自己が管理するパソコンPC11において電子メールソフトS11を起動して、電子メールサーバA1の内容を取りに行く操作を行うことで、ユーザb1の電子メール情報がユーザa1のパソコンPC11に入力される。

【0004】このようにして、ユーザa1が電子メール情報を受け取ると、A社の電子メールサーバA1内の当該電子メール情報は削除されるか、あるいは、保存されたとしてもユーザa1の管理するパソコンPC11内の電子メールソフトS11によって、パソコンPC11内の記憶手段に保存される。

【0005】このように、従来の電子メールシステムでは、あるユーザ宛の電子メール情報は、当該ユーザが管理するパソコン内で管理されることになるため、それを他のユーザが利用するというようなことは通常では行われないのが一般的である。

【0006】しかし、ユーザa1と同じ電子メールサーバA1を用いる他のユーザa2が、B社のユーザb1に電子メールを発信するような場合もある。このとき、ユーザa2は過去にユーザb1と送受信したことがなく、ユーザb1の電子メールアドレスなど通信に必要な情報を知らないとする、ユーザa2はそれらの情報をすべて調べることから始める必要がある。このような場合、ユーザa1がデータとして持っているユーザb1の電子メールアドレスなど通信に必要な情報を他のユーザがそのまま利用できれば手続きが簡単に済む。

【0007】

【発明が解決しようとする課題】しかし、従来の電子メールシステムでは、個々のユーザが持つ様々な情報は、そのユーザが管理するパソコン内に保存されているため、それを他のユーザが利用することは通常では行われず、前述の例の場合、結局は、ユーザa2が受信者であるユーザb1の電子メールアドレスなど通信に必要な情報をすべて調べてそれを打ち込むなどの操作を行う必要があった。

【0008】また、公共のネットワークを介して送られてくる電子メール情報は、コンピュータウイルスに侵されていたり、受信者には配布したくない内容であったりする場合もある。

【0009】しかし、従来の電子メールシステムでは、この種のチェックは何もなされないまま受信者に届けられるので、コンピュータウイルスなどに対する対策は、個々のユーザの管理するパソコンに対して施す必要があり、また、受信者に配布したくないような内容であつて

も、それに対する処理はその電子メール情報を受信したユーザ側で施すしかなかった。

【0010】そこで本発明は、送受信される電子メール情報をシステムが自動的に解析し、その解析結果に基づいて必要な情報をデータベース化して保存することで、通信に必要な情報を、同じ電子メールサーバを用いる複数のユーザが共通に利用できるようにするとともに、電子メール情報の内容をチェックすることで、コンピュータウイルスなどに対する対策をユーザが意識することなく自動的に行うようにすることを目的としている。

【0011】

【課題を解決するための手段】前述した目的を達成するために、本発明の請求項1に記載の電子メール情報管理方法は、少なくとも2つの電子メールサーバ間で送受信される電子メール情報を管理する電子メール情報管理方法において、送受信される電子メール情報の送信時または受信時に、その電子メール情報を解析して、電子メール情報を構成する項目を検出し、その電子メール情報を構成する項目から、或る電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を取り出し、当該電子メールサーバを共通に用いるそれぞれのユーザが管理するそれぞれのコンピュータからアクセス可能に保存するとともに、その電子メール情報を構成する項目のうち、予め定められた項目に対し、その項目に応じた処理を施すようにしている。

【0012】請求項2の発明は、請求項1において、前記或る電子メールサーバを共通に用いるユーザが共通に利用できる情報は、発信者と受信者の少なくとも一方の側の電子メールアドレスとその名前を含み、これらの情報をデータベース化するようにしている。

【0013】さらに、請求項3の発明は、請求項1または2において、前記電子メール情報を構成する項目のうち、予め定められた項目に対しその項目に応じて施す処理は、前記予め定められた項目にコンピュータウイルスが存在するか否かのチェックと、その電子メール情報を受信者に配布すべきか否かを判断するために前記予め定めた項目の内容チェックの少なくとも一方を行い、チェック結果が適正であると判断した場合は、その電子メール情報を前記受け取り側の電子メールサーバに送り、コンピュータウイルスが存在する場合は、コンピュータウイルスの影響を除去したのち、前記受け取り側の電子メールサーバに送り、コンピュータウイルスが除去できない場合、または、前記予め定めた項目の内容が受信者に配布すべきでない内容であると判断された場合は、当該電子メールを削除するようにしている。

【0014】また、請求項4に記載された本発明の電子メール情報管理装置は、少なくとも2つの電子メールサーバ間で送受信される電子メール情報を管理する電子メール情報管理装置において、送受信される電子メール情報を解析して、その電子メール情報を構成する項目を検

出し、その電子メール情報を構成する項目から、或る電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を取り出すとともに、前記電子メール情報を構成する項目のうち、予め定められた項目に対しその項目に応じた処理を施す電子メール情報解析手段と、この電子メール情報解析手段によって取り出された前記或る電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を、これらユーザが管理するそれぞれのコンピュータからアクセス可能に保存するデータ記憶手段とを有した構成としている。

【0015】請求項5の発明は請求項4において、前記電子メール情報解析手段が取り出す当該電子メールサーバを共通に用いるユーザが共通に利用できる情報は、発信者と受信者の少なくとも一方側の電子メールアドレスとその名前であって、これらの情報をデータベース化するようにしている。

【0016】さらに、請求項6の発明は請求項4または5において、前記電子メール情報解析手段が行う電子メール情報を構成する項目のうち、予め定められた項目ごとにその項目に応じて施す処理は、前記予め定められた項目にコンピュータウイルスが存在するか否かのチェックと、その電子メール情報を受信者に配布すべきか否かを判断するために前記予め定めた項目の内容チェックの少なくとも一方を行い、チェック結果が適正であると判断した場合は、その電子メール情報を前記受け取り側の電子メールサーバに送り、コンピュータウイルスが存在する場合は、コンピュータウイルスの影響を除去したのち、前記受け取り側の電子メールサーバに送り、コンピュータウイルスが除去できない場合、または、前記予め定めた項目の内容が受信者に配布すべきでない内容であると判断された場合は、当該電子メールを削除するようにしている。

【0017】また、請求項7に記載の電子メール情報管理処理プログラムを記録した記録媒体は、少なくとも2つの電子メールサーバ間で送受信される電子メール情報を管理する電子メール情報管理処理プログラムを記録した記録媒体であって、その処理プログラムは、送受信される電子メール情報の送信時または受信時に、その電子メール情報を解析して、電子メール情報を構成する項目を検出する手順と、その電子メール情報を構成する項目から、或る電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を取り出す手順と、これによって取り出された情報を、当該電子メールサーバを共通に用いるそれぞれのユーザが管理するそれぞれのコンピュータからアクセス可能に保存する手順と、その電子メール情報を構成する項目のうち、予め定められた項目に対しその項目に応じた処理を施す手順とを含むものである。

【0018】本発明は、送受信される電子メール情報を解析して、電子メール情報を構成する項目を検出し、そ

の電子メール情報を構成する項目から当該電子メールサーバを共通に用いる複数のユーザが共通に利用できる情報を取り出し、これらのユーザがアクセス可能にデータベース化して保存するようにしたので、たとえば、電子メールを送信しようとする相手が過去に送受信したことの無い未知の相手であっても、相手の電子メールアドレスなど送受信に必要な情報をデータベースから簡単に取り出して利用することができ、送受信に必要な様々な情報を調べたりする手間が省け、送受信を行うための処理の効率化が図れる。

【0019】データベース化する情報としては、電子メール情報のヘッダ部に存在する発信者の電子メールアドレスと発信者名、受信者の電子メールアドレスと受信者名などの情報であって、これらの情報をデータベース化することにより、前述したように、同じ電子メールサーバを用いる或るユーザが過去に使った電子メールアドレスなどを、他のユーザが簡単に取り出して利用することができ、電子メールの発信処理の効率化が図れる。さらに、これらの情報を長期間に渡って蓄積することにより、発信者の電子メールアドレスとその名前、受信者のアドレスとその名前などが多数蓄積されることになり、個々のユーザは何等意識することなく自動的に住所録的なデータが作成されることになり、しかも、それを多くのユーザが共通に利用することができるので、きわめて便利なものとなる。

【0020】加えて本発明は、送られてきた電子メール情報を構成する項目のうち、予め定められた項目に対し、その項目に応じた処理を施すようにしたので、従来では、個々のユーザが独自に処理していたことを、本発明では、個々のユーザが何等意識することなくシステム側で自動的に行うことができる。具体的には、電子メール情報の本文部や添付文章部がコンピュータウイルスに侵されているか否かや、その電子メール情報の内容のチェックを行い、コンピュータウイルスに侵されていると判断された場合は、コンピュータウイルスの影響を除去したのち、前記受け取り側の電子メールサーバに送り、コンピュータウイルスが除去できない場合、または、前記電子メール情報の内容が受信者に配布すべきでない内容であると判断された場合は、当該電子メールを削除するようにしたので、本来、受信者が個々に対応すべきコンピュータウイルスに対する処理や電子メール情報の内容のチェックやそれに対する処理が、受信者に届く前の段階でシステム側で自動的に行うことができる。

【0021】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【0022】図1は本発明が適用された電子メールシステムの構成を示すもので、前述した図4と概略的には同じ構成であるが、図1の構成は、電子メールサーバ間で送受信される電子メール情報を解析する電子メール情報

解析部11と、この電子メール情報解析部11で解析された情報のうち、必要な情報（詳細は後述する）を蓄えるデータベース部12が設けられている点が図4と異なる。その他、図4と同一部分には同一符号が付されている。なお、この図1では、電子メール情報解析部11とデータベース部12は、A社側のみ設けられている例を示している。これらはB社側にも設けられてもよいことは勿論であるが、ここでは、説明を簡単にするために、A社側のみについて考えることにする。

【0023】電子メール情報解析部11は、電子メールサーバA1の公共ネットワーク1側に設けられ、送受信される電子メール情報を解析し、必要な情報（詳細は後述する）を抽出して、その抽出した情報をデータベース部12に蓄えるとともに、電子メール情報に対して所定の処理（詳細は後述する）を施すものであるが、この実施の形態では、他の電子メールサーバ（この場合、B社の電子メールサーバB1）から送られてきた電子メール情報を処理する例、つまり、電子メール情報の受信時における処理について説明する。

【0024】また、この電子メール情報解析部11によってデータベース部12に蓄えられた情報は、電子メールサーバA1を共通に用いるユーザa1、a2、a3、・・・の管理するそれぞれのパソコンPC11、PC12、PC13・・・から、それぞれの電子メールソフトS11、S12、S13を起動することによりアクセスできるようになっている。

【0025】ところで、電子メール情報は、一般的には図2に示されるように、ヘッダ部21、本文部22、添付文章部23などにより構成されている。そして、ヘッダ部21には、送信者の名前と電子メールアドレス、受信者の名前と電子メールアドレス、送信経路情報、表題などの情報が存在している。また、本文部22は一般的にはテキスト文章であり、また、添付文章部23はテキスト文章やバイナリ情報による内容となっている。

【0026】次に本発明の処理手順を図3のフローチャートを参照しながら説明する。今、B社のユーザb1がA社のユーザa1に電子メールを送信したとする。その電子メールはB社の電子メールサーバB1により、公共ネットワーク1を介してA社の電子メールサーバA1に対して送られるが、電子メールサーバA1に入る前に電子メール情報解析部11に入る。

【0027】電子メール情報解析部11は、まず、受信した電子メール情報を各項目に分解する（ステップs1）。つまり、電子メール情報は、図2に示されるように、ヘッダ部21、本文部22、添付文章部23などの複数の項目により構成されているため、電子メール情報を受け取ると、ヘッダ部21、本文部22、添付文章部23に分ける。

【0028】そして、ヘッダ部21から必要な情報として、ここでは、発信者の電子メールアドレスと名前、受

信者の電子メールアドレスと名前を抽出して、それをデータベース部12に保存する（ステップs2）。なお、このヘッダ部21には、前述したように、送信者の名前と電子メールアドレス、受信者の名前と電子メールアドレス、送信経路情報、表題などの情報があるが、これらは、たとえば、from:〇〇〇とあれば、〇〇〇は送信者の名前、to:△△△とあれば△△△は受信者の名前というように、電子メールを送受信する際のプロトコル（SMTP:SimpleMail Transfer Protocol）に従って区分することができる。

【0029】その後、本文部22に対し予め決められた処理を施す（ステップs3）。具体的には、本文部22がコンピュータウイルスに侵されているか否かのチェックを行うが、それ以外にも、必要に応じて、様々なチェックを行うことも可能である。たとえば、本文部22の内容をチェックし、その本文部22の内容が仕事上の内容であるか否かを判断し、本来、仕事上の内容が送られてくるべきものが、それとは全く異なる内容である場合、それを発見するなどということも可能である。これは、文章を形態素解析して単語抽出を行うなどして文章を解析し、その解析結果に基づいて、本文部22の内容を判断することができる。

【0030】なお、コンピュータウイルスに侵されていると判断された場合は、それを除去する処理を行う。ただし、コンピュータウイルスの除去ができない場合もある。

【0031】次に、添付文章部23に対し予め決められた処理を施す（ステップs4）。具体的には、本文部22と同様、添付文章がコンピュータウイルスに侵されているか否かのチェックを行い、コンピュータウイルスに侵されていると判断された場合はそれを除去する処理を行うが、前述したように、コンピュータウイルスの除去ができない場合もある。

【0032】以上のステップs1～s4の処理を行ったのち、受信した電子メール情報を削除するか否かを判断する（ステップs5）。具体的には、本文部22と添付文章部23に対しコンピュータウイルスに侵されているか否かのチェックを行い、本文部22と添付文章部23が共にコンピュータウイルスに侵されていないと判定された場合、あるいは、コンピュータウイルスに侵されていてもそれを除去できた場合は、その電子メール情報を電子メールサーバA1に送る（ステップs6）。

【0033】一方、本文部22と添付文章部23の少なくとも一方がコンピュータウイルスに侵されていると判断され、そのコンピュータウイルスの影響を除去できなかった場合は、その電子メール情報を削除する（ステップs7）。

【0034】なお、コンピュータウイルスのチェック以外にも、前述したように、たとえば、仕事上の内容であるか否かをチェックする処理も同時に行う場合には、仕

事上とは全く関係のない内容であって、その電子メール情報を受信者に配布することが適切でないと判断した場合にも、その電子メール情報を削除する。

【0035】このように、受信者に配布することが適切でないと判断したとき、それを削除する処理を設けるのは、今後、電子メールが一般家庭にまでごく普通に普及したような場合に重要なものとなる。たとえば、未成年者などにダイレクトメール的に送られてくる電子メールの中には公序良俗に反するものも含まれると考えられるからである。このような公序良俗に反する内容は、前述したように、内容を形態素解析するなどして、ある程度は判断できるので、これによって、受信者に配布すべきでない内容であるかのチェックは可能となる。

【0036】以上のようなステップs1からs7の処理がなされることにより、まず、データベース部12には、発信者の電子メールアドレスと名前、受信者の電子メールアドレスと名前が保存され、長期間においては、多数の発信者と受信者の電子メールアドレスと名前が蓄えられることになり、住所録的なデータが作成されることになる。

【0037】したがって、たとえば、A社のユーザa2が、B社のユーザb1に電子メールを発信しようとしたとき、ユーザa2は過去にユーザb1と電子メールの送受信をしたことがなく、ユーザb2の電子メールアドレスを自己の管理するパソコン内に持っていなくても、データベース部12の内容を見ることによって、ユーザb1の電子メールアドレスを取り出してそれを利用することができる。

【0038】また、発信者から送られた来た電子メール情報は、受信者に配布される前の段階で、コンピュータウイルスに侵されているか否かのチェックや、その内容がチェックされる。そして、本文部21や添付文章部22がコンピュータウイルスに侵されていると判断された場合は、その影響を除去する処理がなされ、影響を除去できた場合は、その電子メールを電子メールサーバA1に送り、コンピュータウイルスの影響を除去できなかった場合は、その電子メールを削除する処理を行う。また、電子メールの内容が受信者に配布すべきでない内容であると判断した場合は、不要な電子メールであるとして、その電子メールを削除する。

【0039】このように、本発明の実施の形態によれば、従来、個々のユーザが管理していた電子メールアドレスなど電子メールの送受信に必要な様々な情報を、同じ電子メールサーバを利用する複数のユーザが共通に利用可能なデータベース化することができ、しかも、そのデータベース化は個々のユーザが何等意識することなく、システム側によって自動的になされる。これにより、データベース部12に保存されているデータであれば、過去に送信あるいは発信したことがなく、データとして持っていない未知のユーザの電子メールアドレスを

も、直ちに、データベース部12をアクセスすることで取り出すことができる。なお、送信者または受信者の電子メールアドレスとその名前を、データベース部12に格納する際、たとえば、同一アドレスで異なる名前のデータが新たに抽出された場合には、名前が異なっているも、既に保存されている同一アドレスのデータを新たなデータに書き換える。また、同一の名前であってもアドレスの異なるデータが抽出された場合は、既に保存されているデータはそのままにして、新たなデータも保存する。

【0040】また、コンピュータウイルスチェックや電子メール情報の内容チェックなど、従来では、個々のユーザがそれぞれ個々に対処していたものが、ユーザが何等意識することなく自動的に行われるので、ユーザが行うべき処理の負担を大幅に軽減することができる。

【0041】なお、本発明は以上説明した実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲で種々変形実施可能となるものである。たとえば、データベース部12に保存するデータとしては、発信者と受信者の電子メールアドレスやその名前に限られるものではなく、複数のユーザが共通して利用できるデータであれば他のデータでもよい。また、電子メールアドレスとその名前をデータベース化する際、発信者の電子メールアドレスと名前、受信者の電子メールアドレスと名前というように、発信者および受信者の両方の電子メールアドレスとその名前を取り込むことにより、より多くの電子メールアドレスと名前をデータベース化することができるが、これは、発信者と受信者の両方でなく、発信者のみの電子メールアドレスと名前をデータベース化するようにしてもよい。

【0042】また、前記実施の形態では、送られてきた電子メール情報を受信する際に、必要な情報のデータベース化を行ったり、その電子メール情報を構成する項目に対し、その項目に応じた処理を施すということを行ったが、このような処理は、電子メールの送信時に行うことも可能である。

【0043】さらに、本発明は、本文部や添付文書に対するチェック内容も前述の実施の形態で説明したコンピュータウイルスチェックや、仕事上関係のある文書であるか否かだけでなく、種々のチェックが可能であり、そのチェック結果に対する処理を行うことが可能となる。

【0044】また、前述の実施の形態は、図1に示されるように、公共ネットワークを介して接続された異なる2つの会社間で、電子メールの送受信を行う例について説明したが、これは、或る1つの企業や団体内部で、複数の電子メールサーバを設置して、それぞれを内部ネットワークで接続してなるシステムであっても同様に実施することが可能である。

【0045】また、以上説明した本発明の電子メール管

理を行う処理プログラムは、フロッピーディスク、光ディスク、ハードディスクなどの記録媒体に記録させておくことができ、本発明はその記録媒体をも含むものである。また、ネットワークから処理プログラムを得るようにしてもよい。

【0046】

【発明の効果】以上説明したように、本発明によれば、送受信される電子メール情報を解析して、電子メール情報を構成する項目を検出し、その電子メール情報を構成する項目から当該電子メールサーバを共通に用いるユーザが共通に利用できる情報を取り出して保存するようにしたので、たとえば、電子メールを送信しようとする相手が過去に送受信したことのない未知の相手であっても、相手の電子メールアドレスなど送受信に必要な情報をデータベースから簡単に取り出して利用することができ、送受信に必要な様々な情報を調べたりする手間が省け、送受信を行うための処理の効率化が図れる。なお、データベース化する情報としては、電子メール情報のヘッダ部に存在する発信者の電子メールアドレスと発信者名、受信者の電子メールアドレスと受信者名などであって、これらの情報をデータベース化する処理を長期間に渡って行うことにより、やがては発信者の電子メールアドレスとその名前、受信者のアドレスとその名前などが多数蓄積されることになり、個々のユーザは何等意識することなく自動的に住所録的なデータの作成が可能となる。そして、このようなデータを多くのユーザが共通に利用することができるので、きわめて便利なものとなる。

【0047】加えて本発明は、送られてきた電子メール情報を構成する項目のうち、予め定められた項目に対しその項目に応じた処理を施すようにしたので、従来で

は、個々のユーザが独自に処理していたことを、個々のユーザが何等意識することなくシステムが自動的に行うことができる。具体的には、電子メール情報の本文部や添付文章部がコンピュータウイルスに侵されているか否かや、その電子メール情報の内容のチェックを行い、コンピュータウイルスに侵されていると判断された場合は、コンピュータウイルスの影響を除去したのち、前記受け取り側の電子メールサーバに送り、コンピュータウイルスが除去できない場合、または、前記電子メール情報の内容が受信者に配布すべきでない内容であると判断された場合は、当該電子メールを削除するようにしたので、本来、受信者が個々に対応すべきコンピュータウイルスに対する処理や電子メール情報の内容のチェックやそれに対する処理が、受信者に届く前の段階でシステム側で自動的に行うことができる。

【図面の簡単な説明】

【図1】本発明の実施の形態を説明する構成図であり、本発明が適用された電子メールシステムの概略的な構成を示す図。

【図2】電子メール情報の一般的なデータ構成例を示す図。

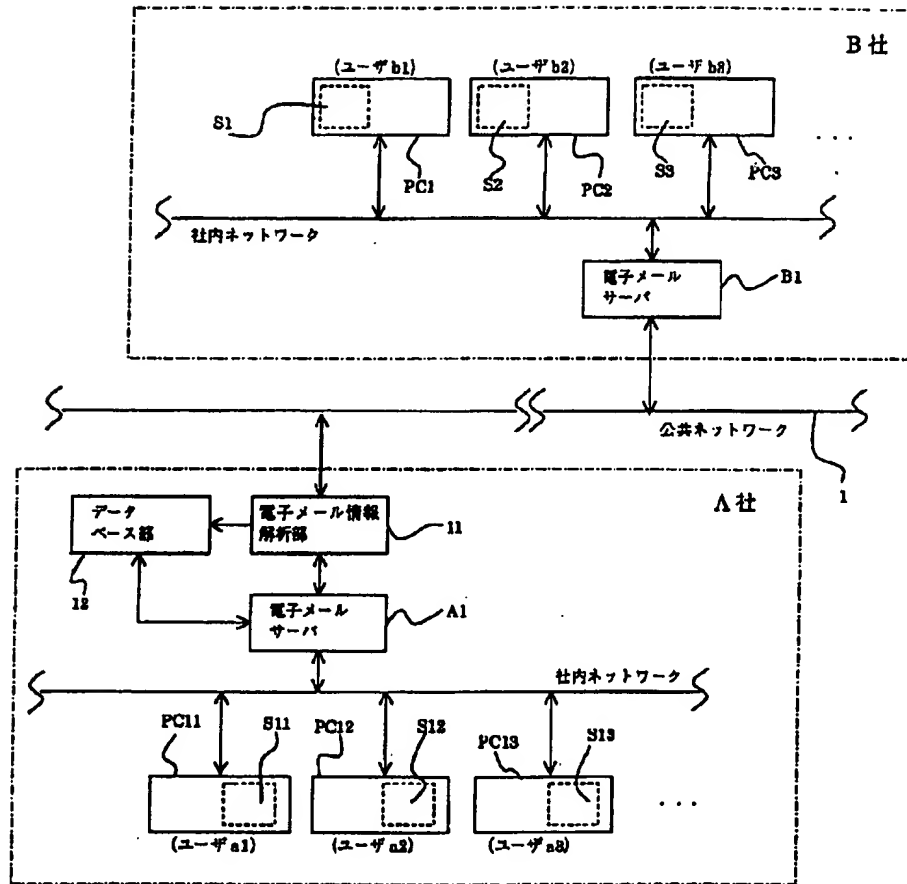
【図3】本発明の実施の形態の処理手順を説明するフローチャート。

【図4】従来の電子メールシステムの概略的な構成図。

【符号の説明】

- 11 電子メール情報解析部
- 12 データベース部
- 21 ヘッダ部
- 22 本文部
- 23 添付文章部
- A1, B1 電子メールサーバ

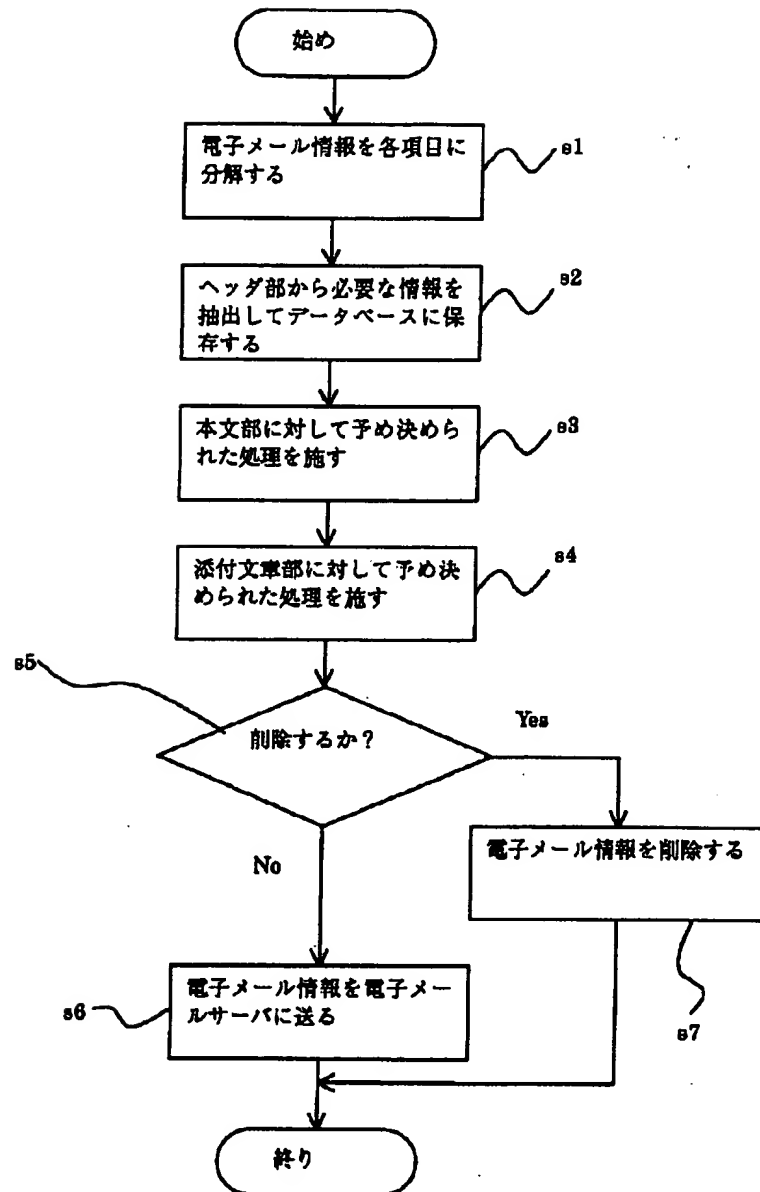
【図1】



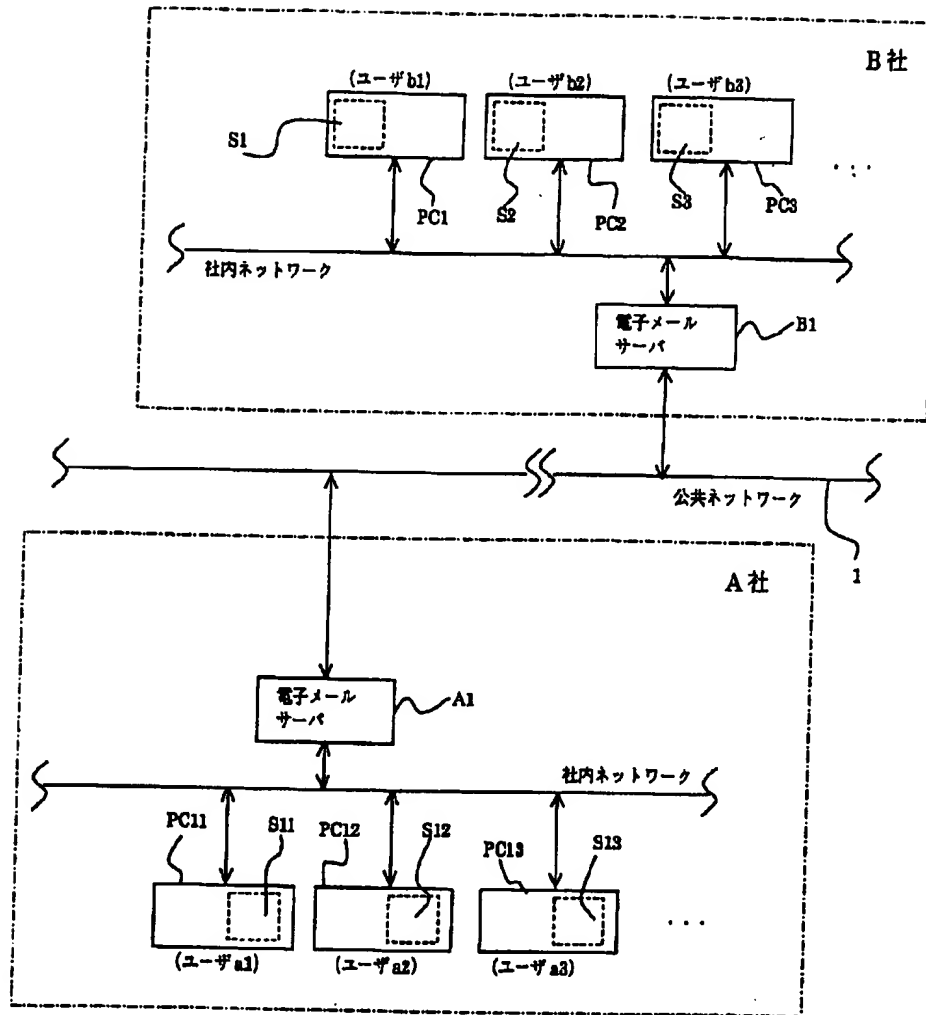
【図2】

21	ヘッダ部	送信者の名前、送信者のアドレス 受信者の名前、受信者のアドレス 経路情報、表題など
22	本文部	テキスト文章
23	添付文章部	テキスト文章あるいはバイナリ情報

【図3】



【図4】



フロントページの続き

(51)Int. Cl.<sup>6</sup>

G 0 6 F 13/00  
17/21  
17/30

識別記号

3 5 1

F I

G 0 6 F 15/20  
15/40

5 9 6 A  
3 1 0 C

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**